JURNAL PINTER
VOL 2. NO.1 JUNI 2018
e-ISSN: 2597- 4475
http://doi.org/10.21009/pinter.2.1.4

# PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN FIREWALL DAN WEB PROXY BERBASIS MIKROTIK DI SMA NEGERI 1 KOTA SUKABUMI

**Garry Tria Irawan[1], M. Djaohar[2], M. Ficky Duskarnaen[3]**

[1] Mahasiswa Prodi Pendidikan Teknik Informatika dan Komputer, Teknik Elektro, FT – UNJ
[2,3] Dosen Prodi Pendidikan Teknik Informatika dan Komputer, Teknik Elektro, FT – UNJ
[1]-geri.tria@yahoo.co.id, [2]-mochamad.djaohar@gmail.com, [3] -duskarnaen@unj.ac.id

**Abstrak**

*Dengan diterapkannya program Cyber School di SMA Negeri 1 kota Sukabumi, maka pelayanan jaringan wajib ditingkatkan. Pelayanan jaringan yang ada saat ini masih belum maksimal terutama pada bagian pemfilteran dan keamanan jaringan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan jaringan menggunakan firewall dan web proxy berbasis Mikrotik. Penelitian yang dilakukan di SMA Negeri 1 Kota Sukabumi bulan Oktober sampai dengan Desember 2014 ini menggunakan metode Research and Development. Membuat aturan firewall dan web proxy selanjutnya menkonfigurasikan aturan tersebut pada router gateway dan pada tahap terakhir akan melakukan uji tes terhadap setiap aturan yang telah dibuat. Konfigurasi yang diterapkan akan menjatuhkan semua aktivitas paket data yang dianggap membahayakan sejumlah port. Memblok paket data menuju router gateway dari jaringan lokal maupun jaringan internet selain administrator. Memblok situs – situs porno dan situs lainnya yang dianggap berbahaya. Hasil uji tes dan scanning yang telah dilakukan didapatkan bahwa firewall dan web proxy telah berhasil mencatat alamat IP yang mencoba memasuki sistem kedalam address-list dan menolak koneksinya. Sehingga kesimpulannya, menerapkan aturan pada firewall dan web proxy telah dapat mengamankan jaringan dari serangan awal cracker.*

**Kata kunci** : **mikrotik, firewall, web proxy, port scanning, brute force**

## 1. Pendahuluan

Perkembangan teknologi jaringan komputer dewasa ini semakin pesat seiring dengan peningkatan kebutuhan masyarakat akan layanan yang memanfaatkan jaringan komputer yang cepat dan efisien dalam lingkungan kerja maupun rumah. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan dan mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian data, perangkat lunak dan peralatan secara bersama. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien.

Peningkatan kebutuhan layanan jaringan komputer telah meningkatkan kerentanan sebuah sistem untuk dapat diserang dari berbagai macam ancaman. Kelemahan dalam sebuah sistem pada program, desain, maupun implementasi dinamakan sebagai *Vulnerability*. Akibatnya timbul suatu ancaman yang dinamakan *Threat,* dan berdasarkan ancaman yang ada, besar kemungkinan terjadi serangan atau *Attack* yang akan mengancam sebuah sistem.

Teknologi firewall dan proxy terus menjadi bentuk paling umum dari perlindungan ancaman yang ada dan ancaman baru terhadap komputer dan jaringan. Pemahaman yang penuh tentang apa yang bisa firewall lakukan, bagaimana firewall dapat digunakan secara maksimal, dan perbedaan antara jenis firewall dapat membuat perbedaan antara integritas jaringan lanjutan dan kegagalan pada komputer atau jaringan.

SMA Negeri 1 Kota Sukabumi adalah sekolah favorit yang menjadi andalan kota Sukabumi yang beralamatkan di jalan R.H. Didi Sukardi No. 124 kota Sukabumi. Rachmat Mulyana, S.Pd, M.Hum selaku kepala sekolah menerapkan program *Cyber School* yang merupakan salah satu program yang baru ditetapkan pada tahun pelajaran 2014/2015 sebagai langkah strategis mendorong peserta didik yang memiliki daya saing dan kemampuan tinggi dalam menghadapi era globalisasi dewasa ini dengan menjalin kerjasama dengan lembaga penyedia sertifikasi internasional dalam bidang informasi.

Pelayanan jaringan di SMA Negeri 1 Sukabumi saat ini masih belum maksimal terutama pada bagian pemfilteran dan keamanan jaringan. Tidak ada peraturan *(Site Security Policy)* yang dibuat kepada pengguna jaringan, tidak ada dokumentasi implementasi jaringan yang dibuat, tidak ada tindakan pencegahan kepada para pengguna jaringan apabila pengguna membuka konten – konten berbahaya atau secara tidak sengaja menyebar



Avalaiable at:
http://journal.unj.ac.id/unj/index.php/pinter/article/view/9769

*malware* ke pengguna lainnya, dan lalu lintas data tidak dimonitoring sehingga jaringan sekolah rentan dan menjadi target banyaknya serangan dari *cracker* iseng yang ingin mencoba memasuki sistem.

Sampai saat ini banyak serangan brute force terhadap router *gateway* SMAN 1 kota Sukabumi dilihat dari *system log* pada router. Pemfilteran menggunaan fitur firewall dan web proxy pada router *gateway* merupakan salah satu solusi agar dapat mencegah serangan awal terhadap jaringan. Laporan ini menyajikan implementasi Mikrotik *Dedicated Router* untuk mengatur lalu lintas data serta melakukan pemfilteran yang dapat menganggu konektifitas jaringan komputer sesuai dengan aturan yang telah ditetapkan dan disepakati bersama.

## 2. Dasar Teori

### 2.1. Mikrotik

Menurut Rendra Towidjojo (2013) Mikrotik adalah kependekan dari "mikrotikls" yang mempunyai arti "jaringan kecil" dalam bahasa Latvia. Mikrotik terbagi menjadi 2 macam tipe, yaitu software (RouterOS) dan hardware (Routerboard). Mikrotik dikenal luas sebagai router. Router adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan, dalam jaringan yang lebih kompleks router digunakan untuk memilih jalan bagi paket data untuk mencapai tujuan.

Menurut Team Citraweb (2014) Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot.

Winbox adalah perangkat lunak yang dirancang khusus untuk mengkonfigurasi router Mikrotik dengan tampilan GUI *(Graphic User Interface)*, perangkat lunak winbox bekerja pada port 8291 dan dapat diunduh secara gratis melalui website *http://www.mikrotik.com/download*.

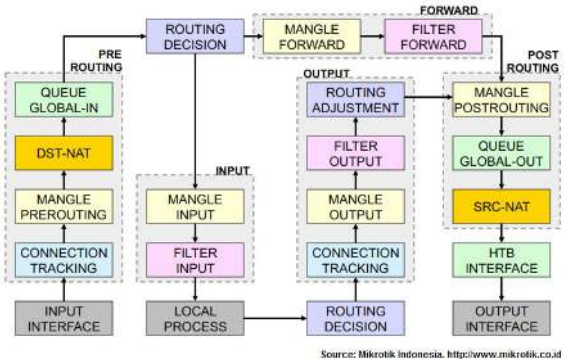
### 2.2. Firewall

Menurut Rendra Towidjojo (2013) firewall merupakan perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan, dengan kemampuan menentukan apakah sebuah paket data bisa masuk dan keluar dari suatu jaringan maka firewall berperan untuk melindungi jaringan dari serangan yang berasal dari luar jaringan, selain ditujukan untuk melindungi jaringan, firewall juga dapat difungsikan untuk melindungi sebuah host atau yang biasa disebut single host.

Setiap paket data memiliki asal (sources) dan tujuan (destination), maka aliran datanya dapat dibedakan menjadi 3 kategori dilihat dari sudut pandang router, yaitu :

1. Dari luar router menuju luar router
2. Dari luar router menuju ke dalam router
3. Dari dalam router menuju ke luar router

Arah aliran paket data yang diproses oleh router dapat dilihat pada gambar 2.1.



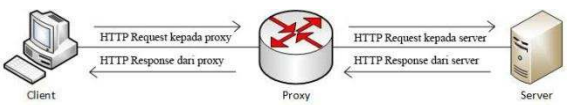

**Gambar 2.1. Arah Aliran Data Pada Router**

Saat merancang firewall, status koneksi dari sebuah paket data harus diperhatikan. Ada 4 status koneksi yang dapat dimiliki sebuah paket data, yaitu:

1. *New,* paket dengan status ini menunjukan bahwa paket tersebut merupakan paket pertama dari sebuah koneksi.
2. *Established,* paket dengan status ini menunjukan bahwa paket tersebut merupakan kelanjutan dari paket new.
3. *Related,* paket ini merupakan paket baru tetapi sebenarnya merupakan kelanjutan dari koneksi yang telah ada sebelumnya.
4. *Invalid,* paket data ini adalah paket yang tidak memiliki hubungan dengan paket lain maupun koneksi lain.

### 2.3. Web Proxy

Menurut Rendra Towidjojo (2013) proxy merupakan aplikasi yang menjadi perantara antara client dan server, sehingga klien tidak akan berhubungan langsung dengan server. Web proxy akan membuat HTTP request ke web server di internet atas permintaan dari komputer user. Sehingga web server akan mengetahui bahwa yang melakukan request adalah proxy server dan bukan komputer user. Contoh ilustrasi pada gambar 2.2.




**Gambar 2.2. Proxy Server**

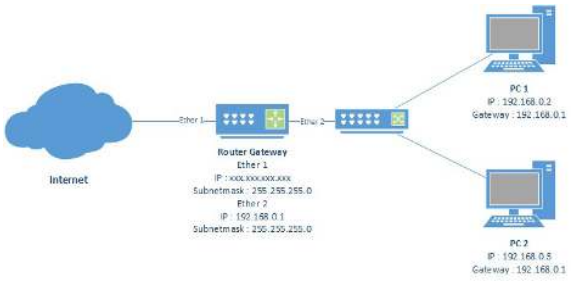
### 2.4. Gateway

Menurut Wildan (2014) *gateway* adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari



Avalaiable at:
http://journal.unj.ac.id/unj/index.php/pinter/article/view/9769

satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda. Istilah *gateway* merujuk kepada hardware atau software yang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga data dapat ditransfer antar komputer yang berbeda-beda. Salah satu contoh penggunaan *gateway* adalah pada email, sehingga pertukaran email dapat dilakukan pada sistem yang berbeda. Pada gambar 2.3 merupakan contoh ilustrasi dari router *gateway* yang ditempatkan diantara jaringan local dan jaringan internet.




**Gambar 2.3. Router Gateway Berada Diantara Jaringan Lokal dan Internet**

## 2.5. Port Scanning

Menurut S'to (2009) scanning merupakan tanda dari dimulainya sebuah serangan, melalui scanning ini penyerang dapat mencari berbagai kemungkinan yang biasa digunakan untuk mengambil alih sistem korban. Scanning adalah Sebuah teknik untuk melihat port yang aktif pada server. Sebuah program port scanning akan mencoba mengirimkan permintaan koneksi pada berbagai rentetan atau daftar port pada server, dan melaporkan kembali port server yang aktif atau merespon balik. Hal ini berguna ketika penyerang tahu kelemahan dari protokol tersebut dan berharap untuk ditemukan untuk selanjutnya akan di eksploitasi. Hal ini juga berguna untuk administrator sistem untuk menentukan tingkat keamanan server dan untuk menguji efektivitas kebijakan akses firewall .

## 2.6. Brute Force

Brute force adalah algoritma yang biasanya digunakan oleh banyak perangkat lunak password cracking. Perangkat lunak password cracker adalah program yang mencoba membuka sebuah password yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang rumit.

# 3. Metodologi

## 3.1. Tempat dan Waktu Penelitian

Penelitian ini dilakukan di Lab Komputer SMA Negeri 1 Kota Sukabumi sejak bulan Oktober 2014 sampai dengan Desember 2014.

## 3.2. Metode Penelitian

Penelitian ini menggunakan metode Research and Development.

## 3.3. Instrumen Penelitian

1. Mikrotik RB1100AHx2 1U Rackmount *(Hardware)*
2. RouterOS v.5.26 *(Software)*
3. Winbox-2.2.18 *(Software)*
4. Nmap – Zenmap *(Software)*
5. Bitvise SSH Client *(Software)*

## 3.4. Prosedur Penelitian

Prosedur penelitian sistem keamanan menggunakan firewall dan web proxy di SMAN 1 Kota Sukabumi tersusun sebagai berikut :

1. Pengumpulan data.
   Pada tahap ini peneliti melakukan observasi terhadap lingkungan sekolah dan wawancara yang dilakukan kepada pihak sekolah untuk mengetahui informasi dasar tentang jaringan komputer yang sudah ada di SMA Negeri 1 kota Sukabumi.
2. Analisis permasalahan.
   Dari hasil observasi dan wawancara, disimpulkan berbagai macam permasalahan yaitu topologi jaringan yang dipakai dapat menyebabkan *Collision Domain, Broadcast Domain*, dan *Data Propagation Delay*, router *gateway* yang digunakan tidak dapat menampung klien dan kebutuhan layanan yang akan digunakan dan tidak ada pengaturan keamanan jaringan oleh administrator.
3. Analisis kebutuhan.
   Selanjutnya penulis melakukan analisis kebutuhan yang menjadi solusi terhadap permasalahan, berupa perangkat *gateway* yang akan digunakan, topologi baru yang akan diterapkan, software yang digunakan untuk melakukan pemblokiran yaitu RouterOS v5.26 dan teknik pemblokiran menggunakan firewall dan web proxy
4. Perancangan system.
   Setelah itu merancang sistem dengan melakukan konfigurasi yang diperlukan agar sistem dapat bekerja sesuai dengan yang diharapkan.
5. Pengujian fungsionalitas system.
   Pada tahap ini, sistem yang telah dikonfigurasi diuji coba fungsionalitasnya apakah sistem bekerja dengan semestinya.
6. Pengujian validitas system.
   Jika sistem sudah bekerja sesuai dengan yang diharapkan, kemudian dilakukan uji validitas terhadap parameter yang digunakan untuk melakukan pemblokiran terhadap serangan yang terjadi.



Avalaiable at:
http://journal.unj.ac.id/unj/index.php/pinter/article/view/9769

7. Analisis data hasil pengujian system.
   Dari hasil pengujian data dianalisis apakah serangan dapat dijatuhkan dengan konfigurasi yang sudah diterapkan.
8. Revisi rancangan system.
   Apabila parameter yang digunakan belum dapat melakukan pemblokiran terhadap serangan yang dilakukan, maka perlu adanya perbaikan pada parameter yang digunakan hingga didapatkan hasil yang sesuai dengan harapan.
9. Menguji rancangan sistem pada jaringan SMAN 1 Sukabumi.
   Setelah dilakukan pengujian fungsionalitas dan validitas pada jaringan kecil dan dianggap layak untuk diterapkan pada sistem yang lebih besar, maka sistem keamanan diterapkan pada *gateway* jaringan dan diuji.
10. Analisis data hasil uji.
    Data dianalisi apakah serangan dapat dijatuhkan oleh sistem yang sudah dirancang.
11. Revisi rancangan system.
    Jika serangan masih bisa dilakukan dan tidak dapat dijatuhkan, maka perlu dilakukan perbaikan hingga sistem keamanan yang dirancang sudah memenuhi kriteria yang diinginkan, kemudian dilakukan penyempurnaan sistem.
12. Implementasi sistem keamanan pada jaringan SMAN 1 Sukabumi.
    Setelah keseluruhan proses revisi sistem telah selesai dilakukan, maka sistem diimplementasikan pada *gateway* jaringan.

### 3.5. Kriteria Penelitian

Kriteria sistem keamanan jaringan di SMAN 1 Sukabumi adalah sebagai berikut :

1. *Unauthorized Access*, merupakan kriteria untuk memberikan akses yang terbatas pada router *gateway* dengan pemberian username dan password sebagai proteksi tingkat rendah hingga pemfilteran pada firewall dan web proxy sebagai proteksi tingkat tinggi yang dapat menampilkan informasi mengenai alamat IP yang berusaha masuk kedalam sistem SMAN 1 Sukabumi menggunakan teknik brute force dan menjatuhkan koneksinya.

2. *Port Scanning Prevention*, firewall dapat melakukan pemblokiran terhadap alamat IP yang melakukan *scanning port* dengan teknik *scanning TCP Connect Scan, TCP SYN Scan, TCP SYN/RST Scan, TCP FIN Scan, TCP SYN/FIN Scan, TCP FIN/PSH/URG Scan, TCP NULL Scan, TCP ACK Scan,* dan *TCP XMAS Scan.*

3. *Safe Content*, web proxy dapat mencegah koneksi klien yang akan membuka konten porno dengan mengalihkan ke web server SMAN 1 Sukabumi. Konten porno selain tidak etis dibuka dilingkungan sekolah dan sering kali menyembunyikan *Trojan, Worm*, dan *Malware* yang membuat klien menjadi DoS Zombie sering kali menjadi isu penting dalam jaringan.

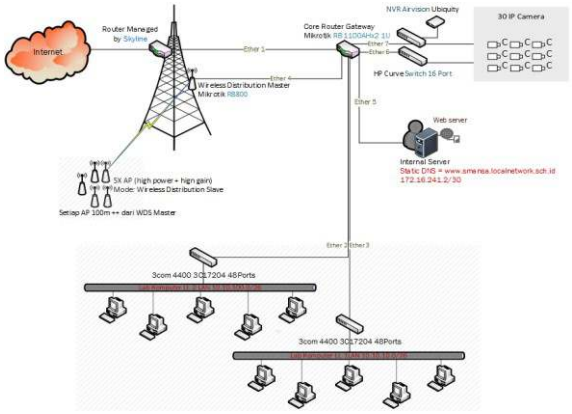
### 3.6. Teknik Analisis Data

Teknik analisis data yang digunakan adalah dengan mengumpulkan data yang didapatkan dari hasil uji konfigurasi dengan metode *stress test.* Pengujian *stress* merupakan pengujian yang didesain untuk melawan sistem dalam keadaan yang tidak normal menggunakan perangkat lunak yang sudah ditentukan, kemudian menentukan keberhasilan konfigurasi dengan melihat *counter-packet* yang bisa dilihat di perangkat lunak winbox.

## 4. Hasil dan Analisis

### 4.1 Analisis Topologi Jaringan

Peneliti harus menganalisis topologi baru yang akan digunakan agar dapat mempermudah dalam menentukan pengalamatan, *interface* yang akan dipakai, konfigurasi firewall, web proxy dan yang lainnya dalam melakukan konfigurasi nantinya. Dari hasil analisis dan diskusi dengan administrator peneliti memutuskan topologi yang akan digunakan adalah sebagai berikut :




**Gambar 4.1. Desain Hasil Analisis Topologi Baru**

### 4.2 Konfigurasi RouterOS

Konfigurasi router gateway meliputi :

1. Konfigurasi Interface
2. Konfigurasi alamat IP
3. Konfigurasi DHCP Server
4. Konfigurasi IP Pool
5. Konfigurasi Routing
6. Konfigurasi DNS
7. Konfigurasi NAT dasar
8. Konfigurasi User
9. Konfigurasi Identitas
10. Konfigurasi Klien NTP
11. Konfigurasi Firewall
12. Konfigurasi Web Proxy

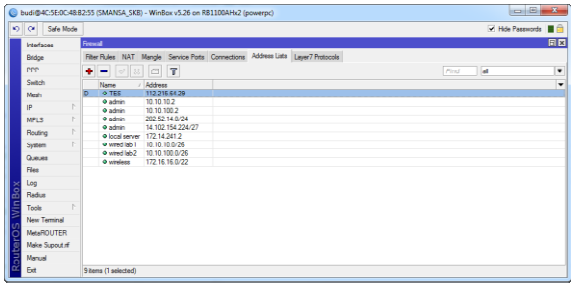
### 4.3 Hasil Pengujian Brute Force

Hasil pemfilteran oleh firewall pada router *gateway* terhadap paket data yang masuk menggunakan protokol TCP pada port



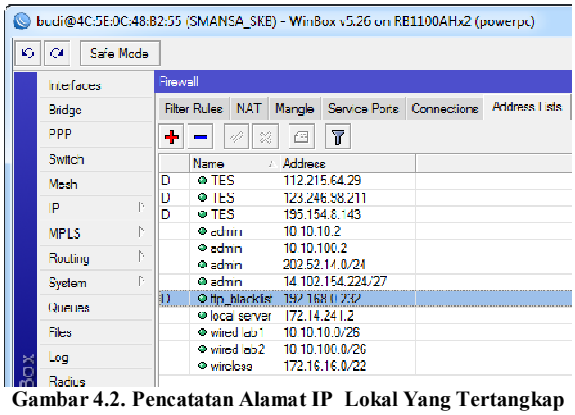
Avalaiable at:
http://journal.unj.ac.id/unj/index.php/pinter/article/view/9769

22,23,80,212,8888, dan 8291 sudah berjalan dengan baik. Firewall sudah dapat mencatat setiap alamat IP yang berusaha masuk melalui port tersebut, hal ini dapat dilihat pada tabulasi *log, address-list*, dan *counter-packet* yang ada disetiap aturan firewall pada perangkat lunak winbox.

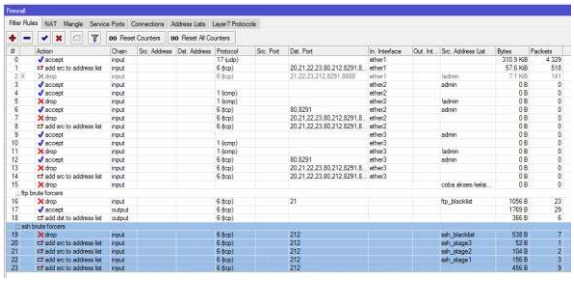


**Gambar 4.1. Pencatatan Alamat IP Publik Yang Tertangkap Oleh Firewall**

Dapat dilihat pada gambar 4.1. dan 4.2 Tanda "D" pada alamat IP TES merupakan kepanjangan dari *"Dynamic"* yang artinya alamat tersebut dicatat secara otomatis oleh firewall.



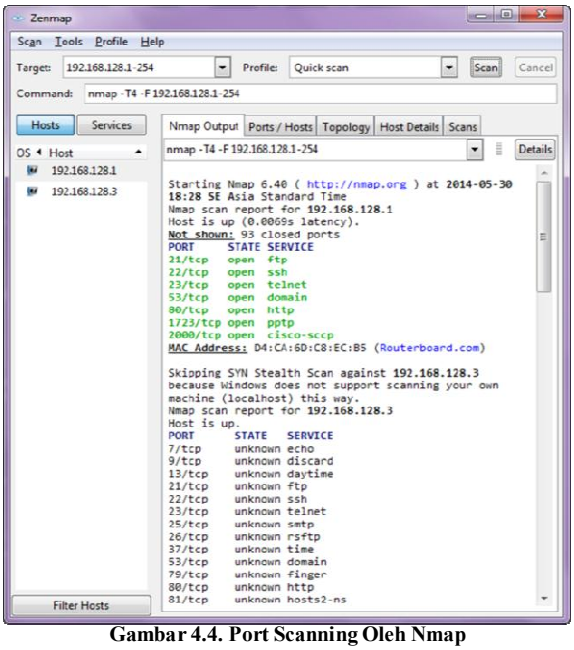
**Gambar 4.2. Pencatatan Alamat IP Lokal Yang Tertangkap Oleh Firewall**



**Gambar 4.3. Counter-Packet menunjukan Rules Firewall Bekerja Dengan Benar**

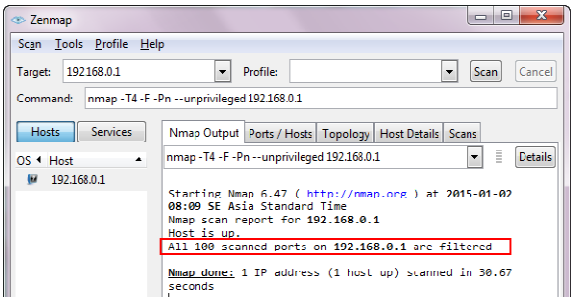
## 4.4 Hasil Pengujian Port Scanning

Sasaran *scanning* adalah alamat IP *interface* router atau jangkauan alamat IP jaringan. Gambar 4.4. adalah gambar *scanning* yang dilakukan oleh nmap terhadap alamat jaringan.



**Gambar 4.4. Port Scanning Oleh Nmap**

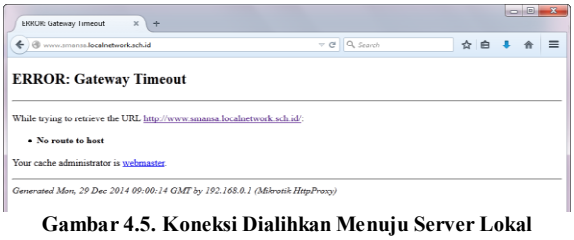
Analisa yang diperoleh berdasarkan hasil scanning pada gambar 4.5. menunjukan bahwa jaringan berada dalam keadaan aman, karena semua port yang dibuka berada dalam kondisi terfilter oleh firewall yang artinya port dalam keadaan tidak terlihat (*stealth*).



**Gambar 4.5. Scanning Terhadap Port Yang Sudah Difilter Dengan Nmap**

## 4.5 Hasil Pengujian Konten Filtering

Penyaringan konten – konten situs porno oleh proxy dengan melakukan pemblokiran pada situs yang didalam URI *(Uniform Resource Identifier)* memiliki kata : *porn, sex, fuck, horny, gay, pussy, babes, ngentot, bokep, xvideos, xhamster, dan redtube.* Koneksi akan dijatuhkan dan dialihkan menuju server lokal. Pengujian dilakukan dengan mencoba mengakses kedalam situs-situs yang memiliki kata tersebut. Jika dilihat dari sisi klien maka akan terlihat seperti gambar dibawah.

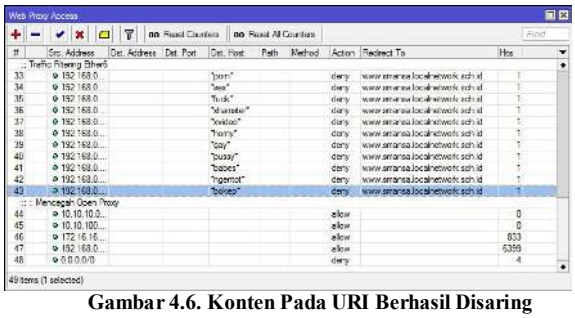



**Gambar 4.5. Koneksi Dialihkan Menuju Server Lokal**



Avalaiable at:
http://journal.unj.ac.id/unj/index.php/pinter/article/view/9769

Dapat dilihat pada Gambar 4.6. dalam tab *Hits*, *counter* yang menunjukan kerja proxy yang sudah dikonfigurasikan bertambah ketika *rules*–nya dijalankan yang menandakan konfigurasi sudah berhasil.



**Gambar 4.6. Konten Pada URI Berhasil Disaring**

## 5. Kesimpulan dan Saran

### 5.1. Kesimpulan

Berdasarkan analisa dari bab – bab sebelumnya dan teori yang ada, maka ditarik kesimpulan bahwa:

1. Pemfilteran paket data menggunakan fitur firewall dan web proxy pada Mikrotik telah menghasilkan laporan pencatatan aktifitas jaringan setiap hari.
2. Pencatatan aktifitas jaringan (logging) yang dihasilkan oleh firewall menggunakan fitur address-list menginformasikan alamat IP komputer penyerang dan dapat digunakan untuk mendeteksi pertanda adanya serangan awal yang ditujukan pada router *gateway*.
3. Hasil pemfilteran paket data pada lalu lintas jaringan menggunakan firewall dan web proxy secara efektif bergantung pada topologi jaringan dan konfigurasi dasar yang diterapkan.
4. Layanan pada nomor port 21,22,23,80,443,8291,8888 dapat dibuka tanpa perlu khawatir adanya serangan.
5. Jenis serangan yang banyak disaring setiap harinya oleh Firewall adalah brute force menggunakan protokol TCP (Transmission Control Protocol) pada lapisan transport dengan alamat IP yang terdeteksi berasal dari China.

### 5.2. Saran

Saran – saran yang dapat penulis berikan berdasarkan hasil analisa dan kesimpulan yaitu :

1. Administrator jaringan harus secara aktif untuk memantau koneksi yang terjadi khususnya koneksi terhadap router *gateway* dengan melihat daftar log dan address-list.
2. Administrator dapat melaporkan alamat IP yang dianggap membahayakan atau secara aktif melakukan serangan terhadap jaringan dengan melacak di situs – situs pencarian alamat IP seperti http://www.whatismyip.com/ip-whois-lookup/ dan mengirimkan email kepada staff ISP (Internet Service Provider) yang bersangkutan agar segera ditindak lanjuti.
3. Alamat IP yang berasal dari jaringan lokal dapat diketahui alamat MACnya untuk dapat diblok secara permanen.
4. Pihak sekolah harus memberikan dorongan dan bantuan pendidikan dan pelatihan bagi SDM, agar kemampuan praktis menjadi lebih berkualitas.

**Daftar Pustaka:**


Cioara, Jeremy, dkk., 2008. *CCNA Examp Prep, Second Edition*. United States of America: Pearson Education, Inc..

Citraweb Nusa Infomedia, 2014. *Mikrotik Training Certified Network Associate (MTCNA)*, Mikrotik Indonesia

Mikrotik Documentation, 2010. Firewall. [terhubung berkala]. *http://wiki.mikrotik.com/wiki/Manual:IP/Firewall*. diambil pada 6 November 2014

Pratama, Wildan. 2014. Perangkat Jaringan. [terhubung berkala]. *http://wildantroubleshoot.blogspot.com/p/pengertian-bridgeswitchhubrouter-dan.html*. diambil pada 15 November 2014

S'to., 2019. *Certified Ethichal Hacker 100% Illegal.* Jakarta : Jasakom

S'to., 2014. *Networking+ illegal.* Jakarta : Jasakom

Shinder, Thomas W., 2003. *MCSA/MCSE Managing and Maintaining a Windows Server 2003 Environment (Exam 70-290): Study Guide and DVD Training System* United States of America: Syngress Media,U.S.

Techopedia, Team. 2014. Secure Network. [terhubung berkala]. *http://www.techopedia.com/definition/24783/network-security*. diambil pada 14 November 2014

Tim Penyusun. 2012. *Buku Pedoman Skripsi/Komprehensif/Karya Inovatif.* Jakarta : Universitas Negeri Jakarta

Towidjojo, R., 2012. *Mikrotik Kung Fu : Kitab 1.* Jakarta : Jasakom

Towidjojo, R., 2013. *Mikrotik Kung Fu : Kitab 2.* Jakarta : Jasakom




Avalaiable at:
http://journal.unj.ac.id/unj/index.php/pinter/article/view/9769